Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and

an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node.

2. (Currently Amended) The system of claim 1 wherein the aggregator determines at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusions.

3. (Currently Amended) The system of claim 2 wherein the aggregator further comprises:

a process that collects statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator.

4. (Previously Presented) The system of claim 1 wherein the aggregator device further comprises:

a process to detect anomalies in connection patterns; and

a process to aggregate detected anomalies into the network events.

5. (Original) The system of claim 1 wherein the collectors have a passive link to devices in the network.

6. (Previously Presented) The system of claim 4 wherein the anomalies include denial of service attacks and scanning attacks.

7. (Previously Presented) The system of claim 4 wherein the anomalies include unauthorized access and worm propagation.

8. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address.

9. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by destination address.

10. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by time.

11. (Original) The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

12. (Original) The system of claim 1 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

13. (Currently Amended) The system of claim ~~1~~ 12 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

14. (Currently Amended) A method, comprises:

sending connection information to identify host connection pairs ~~from~~ collected from a plurality of collector devices to an aggregator; and producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to or from the node.

15. (Previously Presented) The method of claim 14 further comprising:

collecting statistical information in the collector devices to send to the aggregator device.

16. (Currently Amended) The method of claim 15 further comprises:

determining occurrences of network anomalies; and

aggregating anomalies into network events that indicate potential network intrusions and communicating occurrences of network events to an operator.

17. (Original) The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by source address.

18. (Original) The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by destination address.

19. (Original) The method of claim 14 wherein the connection table includes a plurality of records that are indexed by time.

20. (Original) The method of claim 14 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

21. (Original) The method of claim 14 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

22. (Currently Amended) The method of claim 21 ~~14~~ wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other

sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

23. (Original) A method of detecting a new host connecting to a network comprises:

receiving statistics collected from a host in the network; and

indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.

24. (Previously Presented) A method executed in a computing device for detecting a failed host in a network comprises:

determining in the computing device, if both a mean historical rate of server response packets from a host is greater than M and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and

indicating the host as a potential failed host if both conditions are present.